Abstract

A communication network is disclosed such that long messages can be sent from Sender i to Receiver p(i) such that no other receiver can retrieve the message intended for Receiver p(i). The task can easily be completed using interconnection networks and routers. Fast optical networks are slowed down considerably if routers are inserted in their nodes. Moreover, handling queues or buffers at the routers is extremely hard in all-optical setting. A method is disclosed in which the Senders and the Receivers are connected with only a small number of channels (in practice no more than 32 channels); there are no switching or routing-elements in the network, just linear combinations of the signals are computed. Such designs are usable in very fast all-optical networks. The security of the network does not depend on any unproven cryptographical or complexity theoretical assumptions.